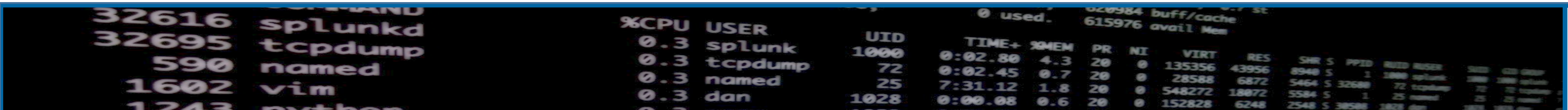
What’s New in Splunk 9.0

Dave Shpritz, Aplura Director of Services

Baltimore Splunk User Group

July 2022

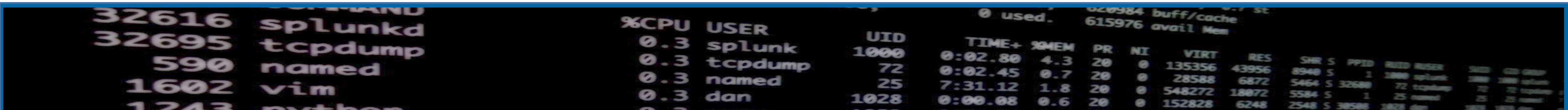


```
32616 splunkd        %CPU USER        UID                0 used.      620984 buff/cache
32695 tcpdump         0.3 splunk     1000   TIME+  %MEM  PR  NI       615976 avail Mem
  590 named           0.3 tcpdump      72 0:02.80   4.3  20   0   VIRT    RES
 1602 vim             0.3 named        25 0:02.45   0.7  20   0 135356  43956
                      0.3 dan        1028 7:31.12   1.8  20   0  28588   6872
                                          0:00.08   0.6  20   0 548272  18072
                                                                152828   6248
```

Many Solutions, One Goal.

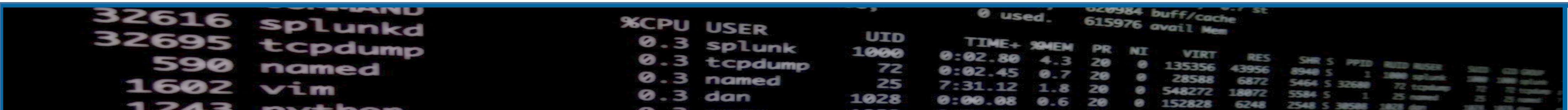
Agenda

- Overview
- Security
- Indexing
- Admin
- Search
- Other stuff

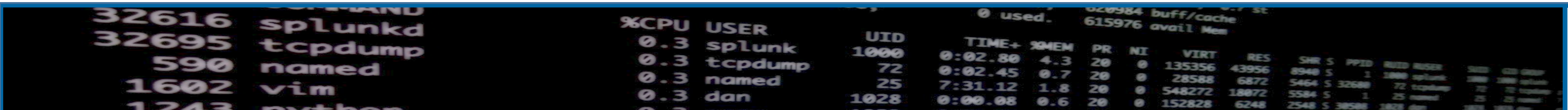


Overview - Splunk Version 9.0.0

- Released at .conf22
- Release Notes: https://docs.splunk.com/Documentation/Splunk/9.0.0/ReleaseNotes/MeetSplunk
- Upgrade: https://docs.splunk.com/Documentation/Splunk/9.0.0/Installation/AboutupgradingREADTHISFIRST
- Known Issues: https://docs.splunk.com/Documentation/Splunk/9.0.0/ReleaseNotes/Knownissues



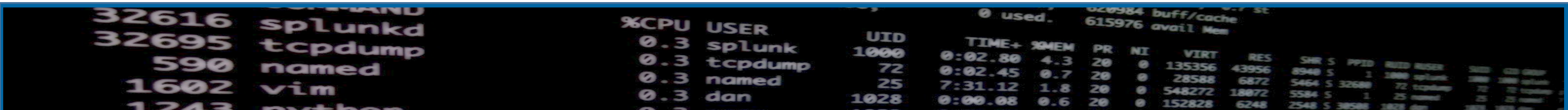
Security



```
32616 splunkd        %CPU USER              0 used.    620984 buff/cache
32695 tcpdump                      UID                 615976 avail Mem
  590 named           0.3 splunk   1000   TIME+  %MEM  PR  NI   VIRT    RES
 1602 vim             0.3 tcpdump    72  0:02.80  4.3  20   0  135356  43956
                      0.3 named      25  0:02.45  0.7  20   0   28588   6872
                      0.3 dan      1028  7:31.12  1.8  20   0  548272  18072
                                         0:00.08  0.6  20   0  152828   6248
```

Security

- Security vulnerabilities
- TLS changes
- Audit improvements/Config Tracking
- Universal Forwarder
- Role-based fields



Vulnerabilities

- Quarterly security patches
- Deployment server/client
  - SVD-2022-0608, SVD-2022-0607
- TLS
  - SVD-2022-0606, SVD-2022-0603, SVD-2022-0602, SVD-2022-0601
- UFs
  - SVD-2022-0605
- Risky commands
  - SVD-2022-0604
- More info:
  - https://www.splunk.com/en_us/product-security.html
  - https://lantern.splunk.com/Splunk_Platform/Product_Tips/Enterprise/Upgrading_Splunk_Enterprise

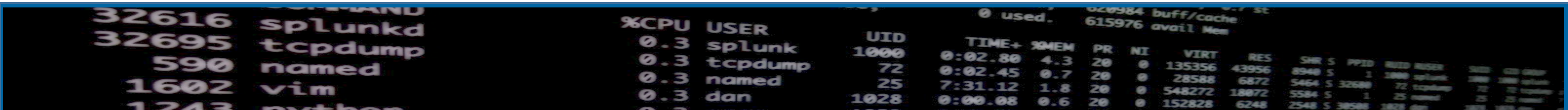
Deployment Server/Client

Deployment servers allow client publishing of bundles (SVD-2022-0608)

- Super bad
- Allows anything on your network to tell the DS to publish an app
- No detection searches
- Mitigate yesterday!
- Backported to 8.1 and 8.2 (the only one of these that was)

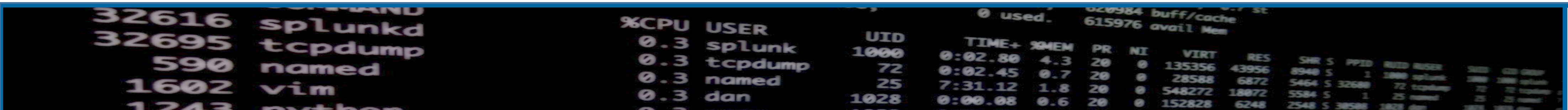
Deployment servers allow unauthenticated bundle access (SVD-2022-0607)

- Anyone can grab apps
- Previous pass4symmkey implementation not effective
- New pass4symmkey, but requires v9 clients
- Certificate validation



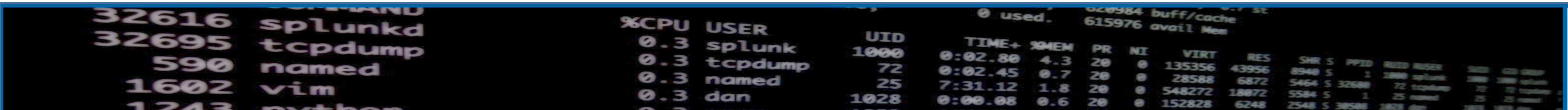
TLS

- SVD-2022-0606, SVD-2022-0603, SVD-2022-0602, SVD-2022-0601
- All present similar issues, that is, Splunk wasn’t validating certificates correctly
- New TLS docs!
- https://docs.splunk.com/Documentation/Splunk/9.0.0/Security/AboutsecuringyourSplunkconfigurationwithSSL



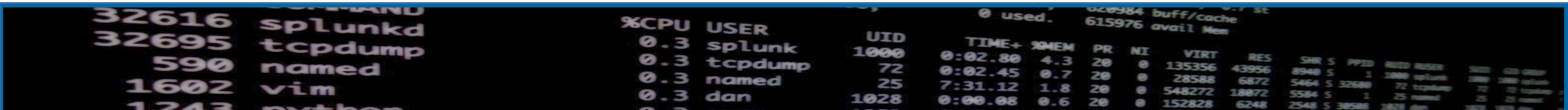
Universal Forwarders

- SVD-2022-0605
- Once you set a password, remote login is allowed by default
- Splunk 9 changes that
- No longer binding to all IPs, just localhost
- You can pull the same trick on older versions



Risky ~~Business~~ Commands

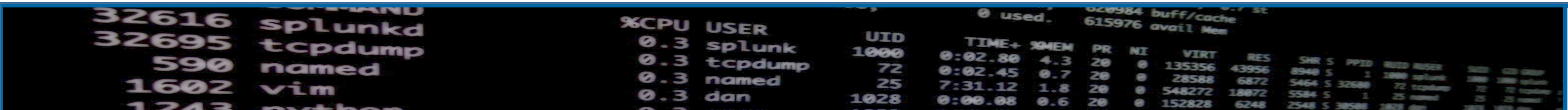
- SVD-2022-0604
- Attacker using a compromised browser could inject commands
- Turn off your GUIs (indexers, for example, maybe your DS)
- New capabilities in Splunk 9



```
32616  splunkd     %CPU USER      UID    TIME+   %MEM
32695  tcpdump      0.3 splunk    1000  0:02.80   4.3
  590  named        0.3 tcpdump     72  0:02.45   0.7
 1602  vim          0.3 named       25  7:31.12   1.8
                    0.3 dan       1028  0:00.08   0.6
```

Audit improvements/Config Tracking

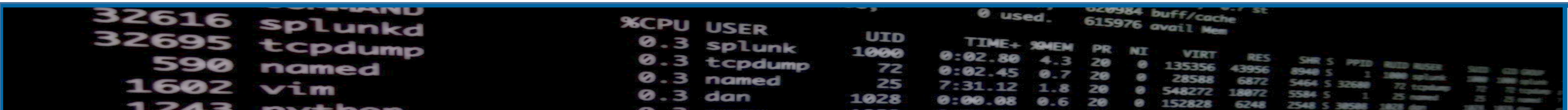
- New internal index, _configtracker, only admin can search by default
- Some fields are ignored, if they are sensitive
- Monitors:
  - $SPLUNK_HOME/etc/system
  - $SPLUNK_HOME/etc/apps
  - $SPLUNK_HOME/etc/users
  - $SPLUNK_HOME/etc/slave-apps
  - $SPLUNK_HOME/etc/instance.cfg
- You can add configs you want ignored
- https://docs.splunk.com/Documentation/Splunk/9.0.0/Troubleshooting/WhatSplunklogsaboutitself#Configuration_Change_Tracker



```
32616  splunkd      %CPU USER      UID
32695  tcpdump       0.3 splunk   1000
  590  named         0.3 tcpdump    72
 1602  vim           0.3 named      25
                     0.3 dan      1028
```

Universal Forwarder Security Improvements

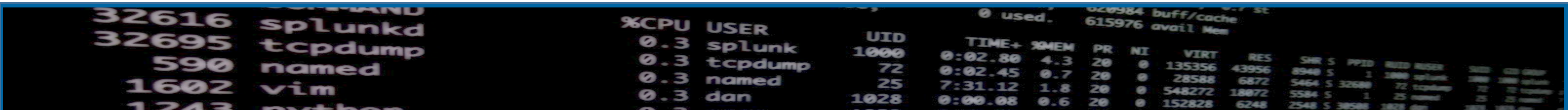
- Config changes now monitored by default
- Windows Managed Service Accounts
- Automatic password generation on Windows
- Linux use of capabilities for a least-privilege install
  - https://docs.splunk.com/Documentation/Forwarder/9.0.0/Forwarder/Installleastprivileged
- Management interface now binds to localhost by default
- Native collection of MacOS Unified Logging



Many Solutions, One Goal.

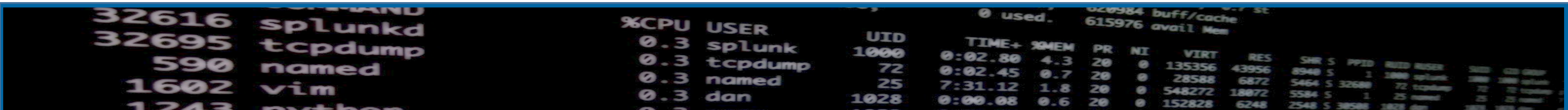
Role-based fields

- Preview feature. Currently provided “as is”, no support
- Can filter or mask
- Allows you to mask fields using SEDCMD-like syntax for obfuscation
- Can replace with hashes to allow for value-based searches/stats
- https://docs.splunk.com/Documentation/Splunk/9.0.0/Security/setfieldfiltering



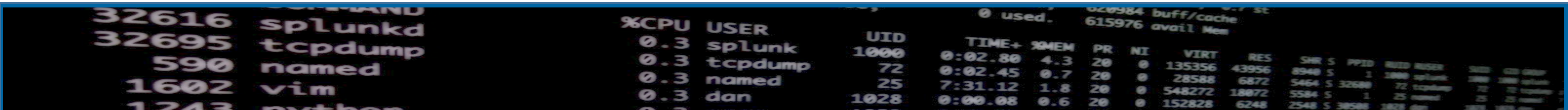
```
32616 splunkd     %CPU USER      UID   TIME+   %MEM
32695 tcpdump      0.3 splunk    1000  0:02.80  4.3
  590 named        0.3 tcpdump     72  0:02.45  0.7
 1602 vim          0.3 named       25  7:31.12  1.8
                   0.3 dan       1028  0:00.08  0.6
```

Indexing



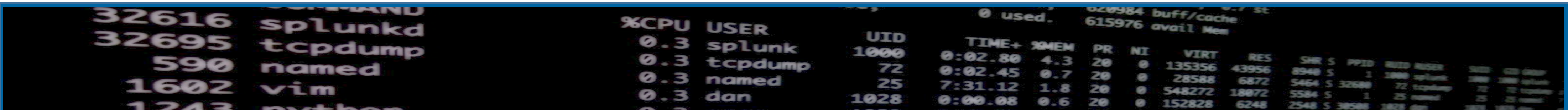
Indexing

- Ingest Actions
- Indexer Manager HA
- Bucket Merging
- Azure SmartStore
- TSIDX compression in SmartStore
- TSIDX writing level



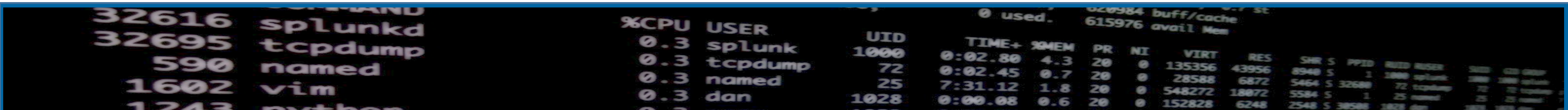
Ingest Actions

- Biggest change to the Splunk pipelines since 7.3
- Allows you more flexibility with data
- You can drop, mask, route (including S3!)
- Competes with Cribl, sort of
- Like TRANSFORMS, SEDCMD, but with a shiny interface (with previews, sometimes)
- Index Manager and Deployment Server deployment methods
- Even works on cooked events!

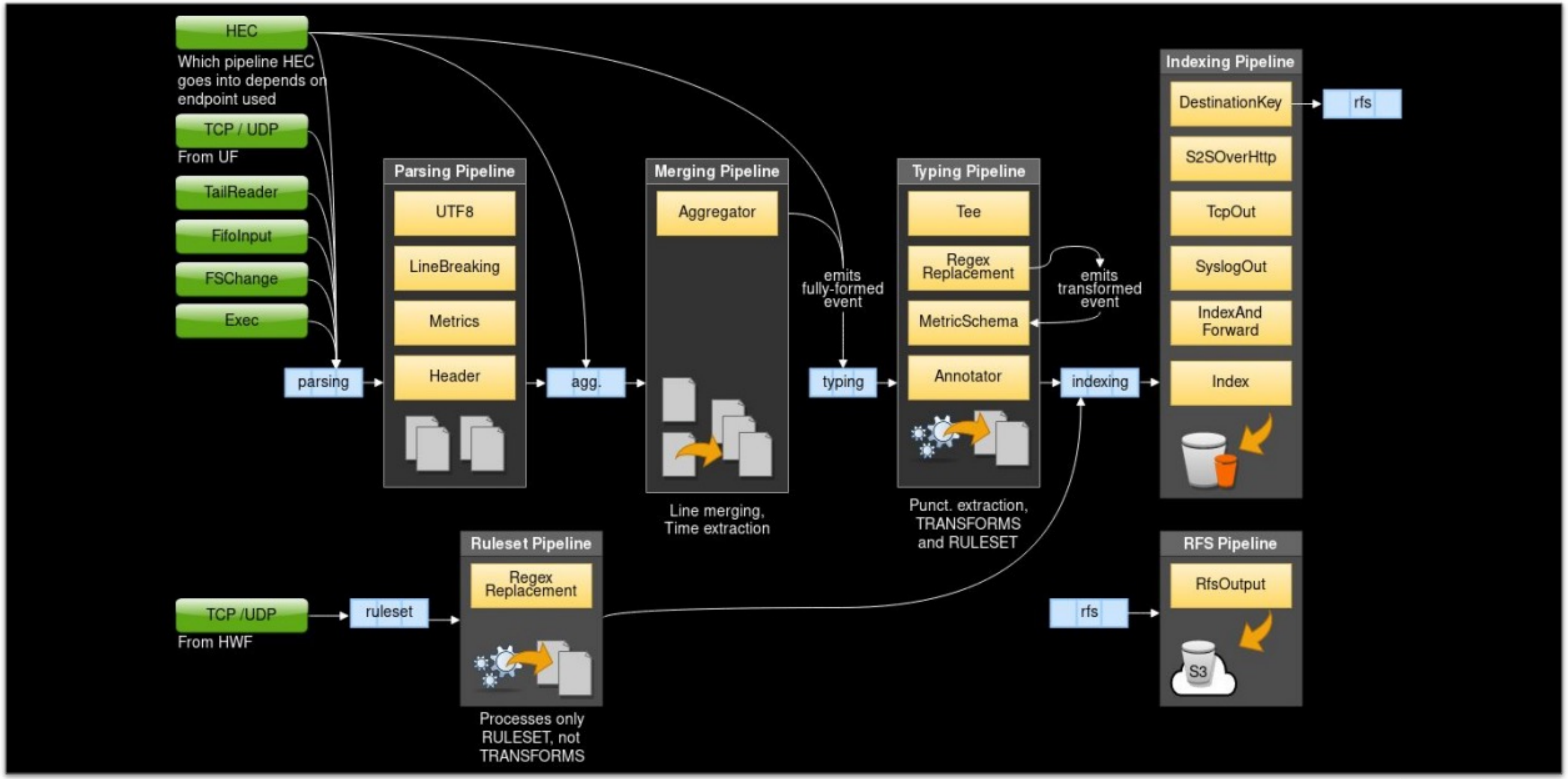


Ingest Actions - pipeline changes

- Uses the existing regexreplace processor
- Also hooked up from the TCP in for cooked events
- Applies after other transforms
- New DestinationKey in indexing pipelines for output to S3
- S3 only works on AWS, saves to a format called ”HEC json”
- Can be used for re-ingest, but no index-time fields other than standard metadata (minus index)
- New metrics (disabled by default, can enable per ruleset)



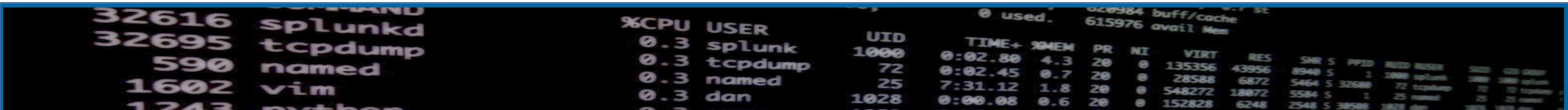
Ingest Actions - the pipelines



From .conf22 **PLA1224A-V**

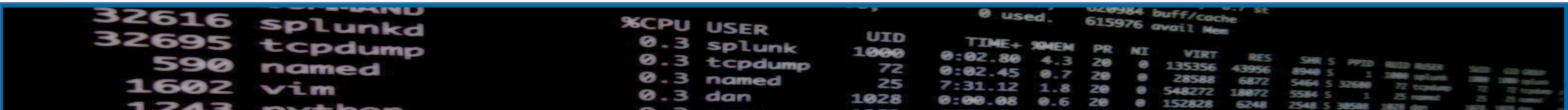
Ingest Actions – Deployment (CM)

- Interface on Cluster Manager allows for preview and deployment
- Interface allows S3 config
- Deployment is just the standard bundle push, so look out for undeployed changes!
- New rulesets don't require rolling restart, but change/remove does (right now)
- New app: splunk_ingest_actions
- New capabilities: list_ingest_ruleset, edit_ingest_ruleset



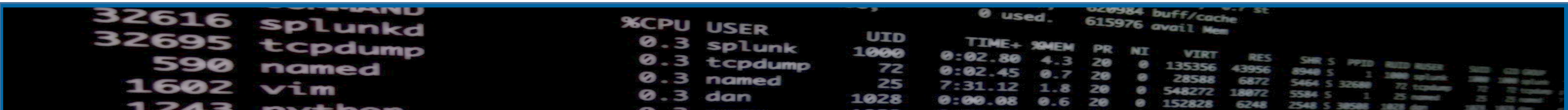
Ingest Actions – Deployment (DS)

- No configuration of S3
- Only supports HF (pipelines may be on UFs, but not tested)
- Currently only supports 10 HFs
- Dedicated DS
- Even visiting the UI creates a new serverclass “IngestAction_AutoGenerated”
- Careful adding rulesets to a TA and then deploying it from your normal DS or to everywhere. Double processing is a thing.



Cluster Manager HA

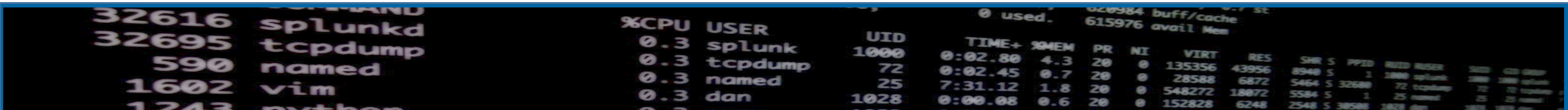
- CM was a single point of failure
- Used to have to sync/failover manually, but some things were in memory, so left behind
- Uses an active/passive topology
- Bundles, generation, peers get synced (bucket list not included)
- Configurable heartbeat
- With a load balancer in front of your CM, this can be automated
- Can also be done with DNS entries, but that would be manual
- New tab in the Indexer Clustering dashboard shows status (in a passive node, that is all you get)
- https://docs.splunk.com/Documentation/Splunk/9.0.0/Indexer/CMredundancy



```
32616  splunkd        %CPU USER            TIME+  %MEM
32695  tcpdump         0.3 splunk   UID   0:02.80  4.3
  590  named           0.3 tcpdump 1000   0:02.45  0.7
 1602  vim             0.3 named     72   7:31.12  1.8
                       0.3 dan       25   0:00.08  0.6
                                   1028
```

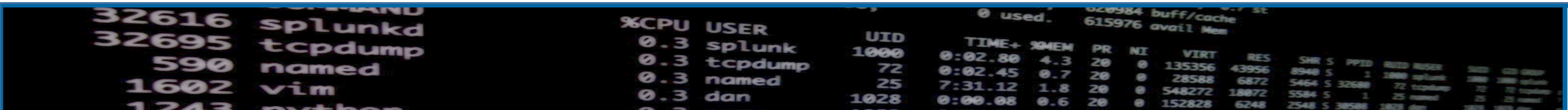
Bucket Merging

- cluster-merge-buckets command
- Can be used to merge smaller buckets for a reduced overall bucket count
- Covers DMA
- Dry run, backup, runtime limitations
- https://docs.splunk.com/Documentation/Splunk/9.0.0/Troubleshooting/CommandlinetoolsforusewithSupport#:~:text=cluster%2Dmerge%2Dbuckets,the%20old%20buckets%20are%20removed



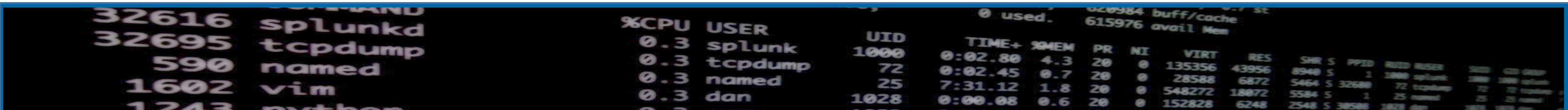
Azure SmartStore

- SmartStore (S2) now can be done natively in Azure
- Uses Azure Blobs
- Not a ton of docs
- https://docs.splunk.com/Documentation/Splunk/9.0.0/Indexer/ConfigureAzureremotestoreforSmartStore#Configure_an_Azure_Blob_remote_store



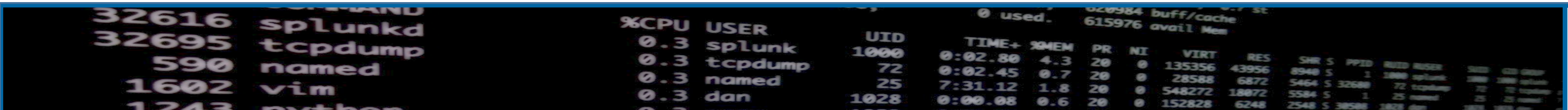
TSIDX compression in SmartStore

- Save storage space/transit for S3
- Compression/decompress is transparent, done on the wire
- Average compression ratio is 50%
- Basic config, just need to turn it on
- Only works on AWS S3
- Once you have turned it on, you cannot turn it off, no backing down (remember, downgrade isn’t a supported thing)
- “Talk to support first”
- https://docs.splunk.com/Documentation/Splunk/9.0.0/Indexer/ConfigureSmartStore#Compress_tsidx_files_upon_upload_to_S3

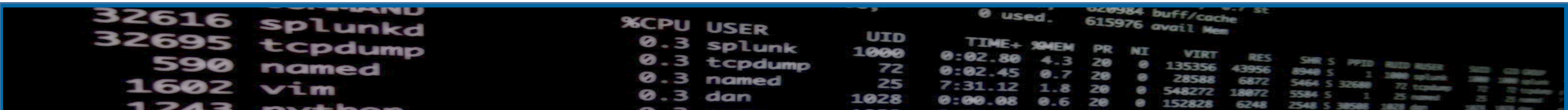


TSIDX writing level

- Controls the format of the TSIDX files
- Enhancements have been made over the years, version dependent
- Now defaults to 3 (was 2)
- Max is 4
- Older indexers can't read the newer levels
- Check the chart in docs for version compatibility
- https://docs.splunk.com/Documentation/Splunk/9.0.0/Indexer/Reducetsidxdiskusage#The_tsidx_writing_level

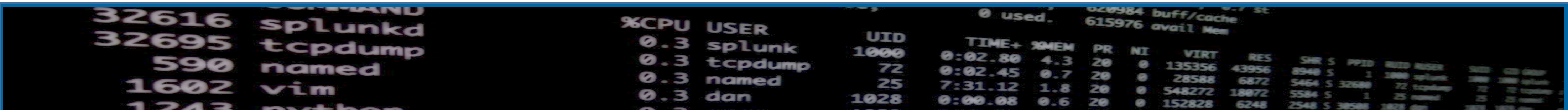


Admin



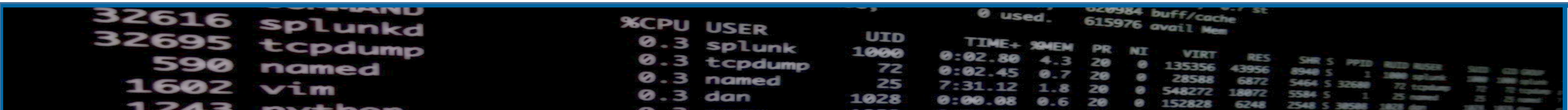
Admin

- Splunk Assist
- KVStore upgrade
- Readiness App and Python 3
- Health Report and Monitoring Console
- Workload management
- Biased Language



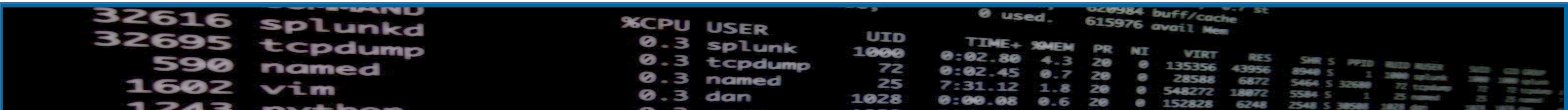
Splunk Assist

- Cloud based service, can be used from on-prem
- Uses telemetry data, so you have to be sending that (Usage Data)
- Net new offering
- In the Monitoring Console
- Needs to be activated
- Tied to your enterprise license
- Can't be used on FIPS instances or in docker
- Current features:
  - TLS cert checking is a feature that jumps out: https://docs.splunk.com/Documentation/Splunk/9.0.0/DMC/UseCertAssist
  - Config assist: https://docs.splunk.com/Documentation/Splunk/9.0.0/DMC/UseConfigAssist



KVStore upgrade

- Migrates from KVStore version 3.6.x to 4.2
- Reduces storage usage
- Performance improvements
- Upgrading to 9 requires this
- Also requires upgrading to WiredTiger, if you haven’t already
- Automatic if you upgrade to 9
- https://docs.splunk.com/Documentation/Splunk/9.0.0/Admin/MigrateKVstore#Migrate_the_KV_store_storage_engine



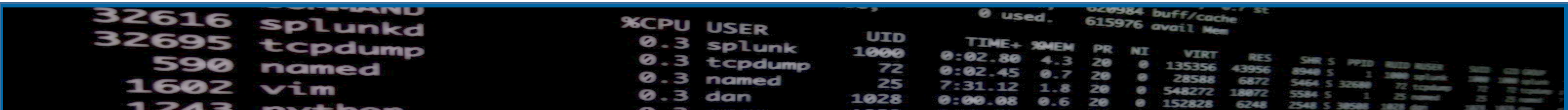
```
32616  splunkd         %CPU USER      UID
32695  tcpdump          0.3 splunk    1000
  590  named            0.3 tcpdump     72
 1602  vim              0.3 named       25
                        0.3 dan       1028
```

APLURA

Many Solutions, One Goal.

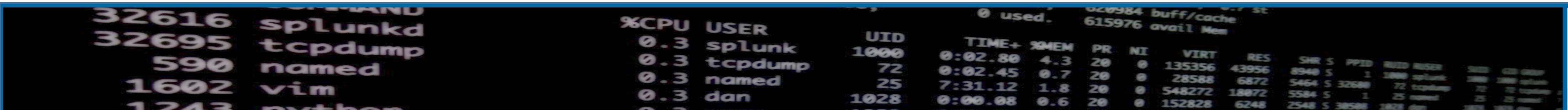
Readiness App and Python 3

- Splunk Upgrade Readiness App now at version 4
- Prepares for Python 3 and jQuery framework changes
- Can scan for issues
- There is no Python 2 in Splunk 9
- Checks TLS configurations (inbound and outbound in Python)
- https://docs.splunk.com/Documentation/Splunk/9.0.0/UpgradeReadiness/About



Health Report and Monitoring Console

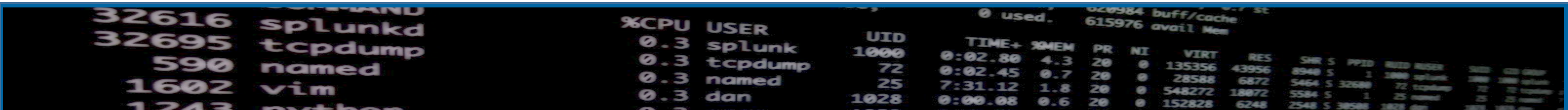
- Better descriptions of indicators and what they mean
- New forwarder latency indicator
- Also looks for potential config issues
- Alerts can now be snoozed
- Alerts can be emailed to admins
  - https://docs.splunk.com/Documentation/Splunk/9.0.0/DMC/Configurealerts#Set_up_health_report_alert_actions
- Monitoring Console now can automatically build your asset list
  - https://docs.splunk.com/Documentation/Splunk/9.0.0/DMC/Configureindistributedmode#Enable_automatic_distributed_mode_configuration



```
32616  splunkd          %CPU USER      UID     TIME+   %MEM
32695  tcpdump           0.3 splunk   1000   0:02.80   4.3
  590  named             0.3 tcpdump    72   0:02.45   0.7
 1602  vim               0.3 named      25   7:31.12   1.8
                         0.3 dan      1028   0:00.08   0.6
```

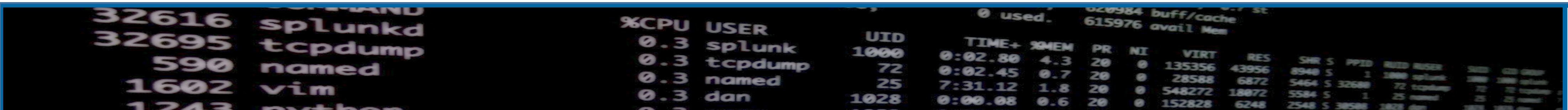
Workload management

- More options for more flexibility
- Roles and indexes now support wildcards
- Can set limits on Ad doc searches
- https://docs.splunk.com/Documentation/Splunk/9.0.0/Workloads/WorkloadRules



Biased Language

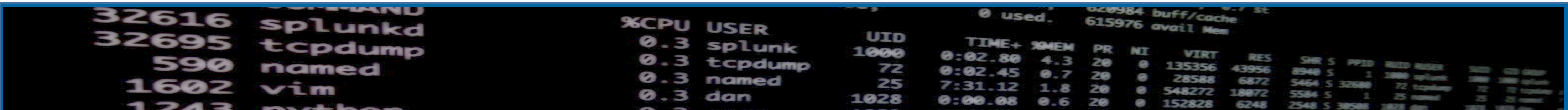
- This has been a long running project at Splunk
- Started a few releases ago
- IDXC, Licensing, allow and deny lists
- There is backwards compatibility, but older config directives may be removed, there are a lot of notes in the docs around this
- Note that you can't use both
- Path changes: master-apps -> manager-apps, slave-apps -> peer-apps
  - https://docs.splunk.com/Documentation/Splunk/9.0.0/Indexer/Updatepeerconfigurations#Which_directory_to_use:_manager-apps_or_master-apps.3F
- The old terms still remain in logs as there are customers that use them in multiple ways. Logging may change once more of the effort is complete
- In MC, there are server roles that may need to be updated



Search

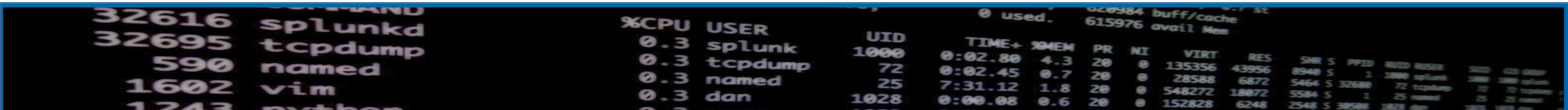
Search

- Federated Search
- Geoip DB



Federated Search

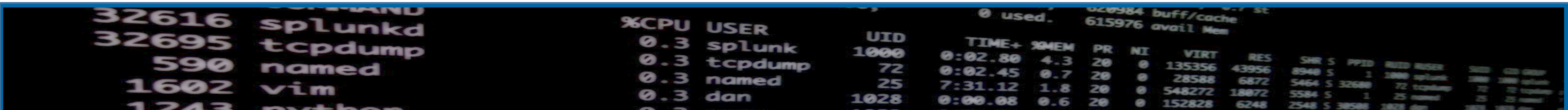
- Federated Search != Hybrid Search: http://docs.splunk.com/Documentation/Splunk/9.0.0/Search/Hybrid2Federated
    - Hybrid = peering to other CM/indexers
    - Federated Search = connecting via remote SH
- https://docs.splunk.com/Documentation/Splunk/9.0.0/Search/Aboutfederatedsearch
- Better UI with options for restrictions for knowledge objects to limit bundle replication
- Now options for Splunk Cloud -> On prem FS
- Can now use tstas, data models, DMA, lookups
- Transparent Federated Search
    - No more writing in special commands or syntax
    - Only runs in fast mode, so no search-time fields
    - No real-time searching
    - Has to be Transparent or Standard mode, not mixed



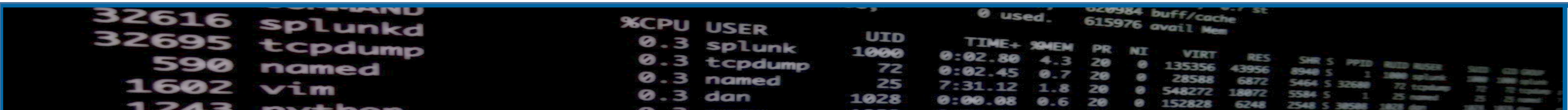
```
32616  splunkd        %CPU USER
32695  tcpdump         0.3 splunk
  590  named           0.3 tcpdump
 1602  vim             0.3 named
                       0.3 dan
```

Geoip DB

- No longer using MaxMind as the provider
- The format is the same
- Now using an open source provider
- If you are using a subscription from MaxMind, it will still work



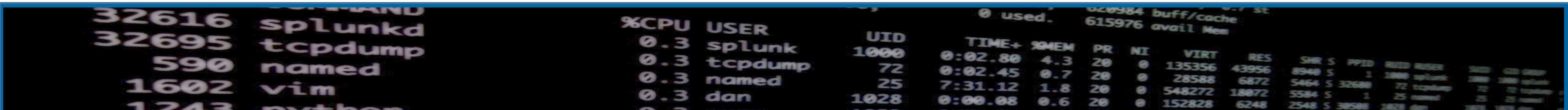
Other stuff



```
32616 splunkd      %CPU USER           0 used.   620984 buff/cache
32695 tcpdump       0.3 splunk    UID            615976 avail Mem
  590 named         0.3 tcpdump  1000  0:02.80  4.3  20  0  135356  43956
 1602 vim           0.3 named      72  0:02.45  0.7  20  0   28588   6872
                    0.3 dan        25  7:31.12  1.8  20  0  548272  18072
                                 1028  0:00.08  0.6  20  0  152828   6248
```

Other stuff

- Dashboards
  - Syntax changes for visualizations
  - No more inline stylesheets
  - Lots of changes to Dashboard Studio: https://docs.splunk.com/Documentation/Splunk/9.0.0/DashStudio/WhatNew
- jQuery
  - Admins can disable jQuery 2 access
- Splunk Secure Gateway App
  - New version, lots of changes to make mobile access better
- Semantic versioning of APIs
  - Makes writing things using Splunk APIs easier and more stable, allows for targeting a specific version, and gentle deprecation of older versions
  - https://semver.org/



```
32616  splunkd        %CPU USER
32695  tcpdump         0.3 splunk
  590  named           0.3 tcpdump
 1602  vim             0.3 named
                       0.3 dan
```